Security Architecture Narrative

IronHub Inc

August 2026

Contents

1 Security Architecture Narrative **3**

2 IronHub Product Architecture **3**

3 IronHub Infrastructure **3**
3.1 Product Infrastructure 3
3.1.1 Authorized Personnel 4
3.2 IT Infrastructure 4

4 IronHub Workstations **4**
4.1 Remote Access 4

5 Access Review **5**

6 Vulnerability Management **5**

7 Penetration Testing **5**

8 IronHub Physical Security **5**

9 Risk Assessment **5**
9.1 Adversarial Threats 6
9.2 Non-Adversarial Threats 6

10 References **6**
10.1 Narratives 6
10.2 Policies 7
10.3 Procedures 7

Table 1: Control satisfaction

Standard	Controls Satisfied
TSC	CC6.6, CC6.7, CC7.1, CC7.2

Table 2: Document history

Date	Comment
Jun 1 2018	Initial document
Apr 21 2026	Updated with IronHub infrastructure, threat inventory, and controls

1 Security Architecture Narrative

The following describes the security architecture of IronHub and how it satisfies the applicable Trust Services Criteria related to logical and physical access controls, system monitoring, and vulnerability management.

2 IronHub Product Architecture

IronHub provides a white-labeled digital home-buying platform hosted on Heroku and AWS. The platform is a multi-tenant SaaS application with strong logical separation of customer data. The platform exposes a web application to home-builders and their prospective buyers, and integrates with third-party services for identity verification, credit reporting, digital document execution (DocuSign), and payment processing.

All communication between clients and the IronHub platform is encrypted in transit using TLS 1.2 or higher. Customer data is encrypted at rest using AES-256 via Heroku Postgres and AWS S3 managed encryption.

3 IronHub Infrastructure

3.1 Product Infrastructure

IronHub's production infrastructure consists of the following components:

Component	Provider	Purpose
Application Host	Heroku	Application and API hosting
Primary Database	Heroku Postgres	Production relational database
Cache	Heroku Redis	Session and data caching
File Storage	AWS S3	Secure storage for documents and uploaded files
Identity & Access	AWS IAM	Cloud access management
DNS / WAF	Cloudflare	DNS, DDoS protection, and Web Application Firewall
Monitoring	DataDog	Infrastructure monitoring, alerting, and anomaly detection
Error Tracking	Rollbar	Application error tracking and log aggregation

3.1.1 Authorized Personnel

- **Heroku** administrative access is granted only to the CTO and designated senior engineers
- **AWS root account** access is granted only to the CTO and CEO
- **AWS IAM** access is granted to a limited group of Operators with least-privilege roles
- **Production database** access is granted only to the CTO and senior engineers via secure VPN
- **Cloudflare** administrative access is restricted to the CTO and IT staff

3.2 IT Infrastructure

IronHub uses the following cloud services for its internal operations:

- Google Workspace (email, calendar, documents)
- JIRA (project management and ticketing)
- Zoho Desk (customer support management)
- Slack (internal communications)
- Bitbucket (source code management)
- 1Password (credential and secrets management)
- Cloudflare (DNS, WAF, and DDoS protection)

Access to these services is provisioned through SSO where available, and is reviewed quarterly as well as via onboarding and offboarding procedures for new and departing personnel.

4 IronHub Workstations

IronHub-issued workstations are hardened against logical and physical attack by the following measures:

- Operating system must be within one generation of current (macOS or Windows)
- Full-disk encryption enabled (FileVault on macOS; BitLocker on Windows)
- Endpoint antivirus/antimalware software installed and active
- Operating system and security software automatically updated
- Screen lock enabled with a timeout of 5 minutes or less

Workstation compliance with these measures is evaluated on a quarterly basis via the Collect Workstation Details procedure.

4.1 Remote Access

IronHub employees regularly work remotely. Remote access to production systems is restricted to authorized personnel via encrypted connections (SSH or VPN). Employees are responsible for ensuring that only authorized individuals have physical or logical access to IronHub-issued devices and systems.

5 Access Review

Access to IronHub infrastructure, both internal and product-facing, is reviewed quarterly. Inactive accounts are removed and anomalous access patterns are reported to the ISM for investigation. When employees join or depart, the onboarding or offboarding procedure is followed to provision or deprovision access accordingly.

6 Vulnerability Management

IronHub conducts automated vulnerability scans of external-facing systems monthly and internal systems quarterly, using industry-standard scanning tools. Findings are reviewed by the ISM within 5 business days of scan completion and remediated according to the SLAs defined in the Vulnerability Management Policy:

Severity	CVSS Score	Remediation SLA
Critical	9.0–10.0	7 days
High	7.0–8.9	30 days
Medium	4.0–6.9	90 days
Low	0.1–3.9	180 days

7 Penetration Testing

IronHub commissions an external penetration test of its production environment at least annually, performed by a qualified third-party security firm. All findings are reviewed by the ISM and Leadership Team and tracked to remediation.

8 IronHub Physical Security

IronHub's primary office is located at #300, 207 9th Ave SW, Calgary, AB T2P 1K3. Physical access to the office is controlled via key issuance tracked in the Office Physical Security Policy Ledger. IronHub managers regularly review physical access privileges.

IronHub's production infrastructure is hosted entirely within Heroku and AWS cloud environments. IronHub does not maintain or operate physical data center hardware.

9 Risk Assessment

IronHub updates its Cyber Risk Assessment on an annual basis to keep pace with the evolving threat landscape. The following is an inventory of adversarial

and non-adversarial threats assessed to be of importance to IronHub.

9.1 Adversarial Threats

Threat	Source	Vector	Target	Likelihood	Severity
Phishing / Social Engineering	External actors	Email, SMS	Employees	High	High
Ransomware	Cybercriminals	Phishing, unpatched systems	Workstations, servers	Medium	Critical
Credential compromise	External actors	Phishing, credential stuffing	Cloud accounts, SaaS	High	High
Unauthorized data access	Insider / external	Misconfigured access controls	Production database	Low	Critical
Supply chain compromise	Third-party vendor	Vulnerable dependencies	Application code	Low	High
Funds transfer fraud	External actors	Business email compromise	Finance team	Medium	High
DDoS attack	External actors	Network flood	Platform availability	Low	Medium

9.2 Non-Adversarial Threats

Threat	Vector	Target	Likelihood	Severity
Cloud provider outage	Third-party infrastructure failure	Platform availability	Medium	High
Data loss / corruption	Software bug, accidental deletion	Production database	Low	High
Misconfiguration	Human error in deployment	Cloud infrastructure	Medium	Medium
Hardware failure	End-of-life workstation	Employee productivity	Medium	Low
Employee error	Inadequate training	Data handling, access	Medium	Medium

10 References

10.1 Narratives

- Products and Services Narrative

- System Architecture Narrative
- Organizational Narrative

10.2 Policies

- Encryption Policy
- Log Management Policy
- Office Security Policy
- Remote Access Policy
- Security Incident Response Policy
- Vulnerability Management Policy
- Workstation Policy
- Asset Management Policy
- Security Awareness Training Policy

10.3 Procedures

- Apply OS Patches
- Review and Clear Low-Priority Alerts
- Review Access
- Review Devices and Workstations
- Vulnerability Scan (External and Internal)
- Penetration Test